REMARKS

After the foregoing amendment, claims 9-16 are pending in this application. Claims 1-8 have been cancelled and the subject matter thereof has been incorporated into new claims 9-16. Support for the new claims can be found throughout the specification. Accordingly, no new matter has been added to the application as a result of the entry of new claims 9-16.

Prior Art Rejections

1. Claims 1, 2, 4 and 6-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan *et al.*). The Examiner takes the position that Herve teaches a method of producing a response with a device comprising an input for receiving an input, calculation means for producing a response which is responsive to the input and a secret key by utilizing a first predetermined function. The Examiner further suggests that the Dolan *et al.* patent teaches the features of the claims not taught by Herve, namely, storing in a memory of the device a key-specific number and a coded key which is calculated by means of the secret key, the key-specific number and a device-specific second predetermined function and, when producing the response, reading the key-specific and the coded key from the memory, calculating the secret key on the basis of the key-specific number and a coded key by using the inverse function of the second predetermined function and utilizing the calculated secret key to produce the response. The Examiner concludes that it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the feature of Dolan *et al.* into the system of Herve and that motivation to make the combination is found in column 2, lines 10-40 of Dolan *et al.* For the reasons set forth in detail below, the Applicant respectfully traverses the rejection as it may be applied with respect to new claims 9, 10, 12, and 14-16 which are similar in scope to the rejected claims.

New claims 9-16 have been added in order to more particularly point out and distinctly claim the patentable aspects of the invention. In particular, new claims 9-16 are specifically directed to a method of producing a response with a smart card (claims 9-11), a smart card (claims 12-13) and a system comprising a smart card (claims 14-16). Claims 9-16 all emphasize the fact that a smart card is involved and that the various method steps and operations take place within the smart card itself. As discussed in greater detail below, utilizing a smart card to perform the necessary calculations using a coded key is believed to not be disclosed, taught or suggested by the prior art.

The present invention comprises a smart card and related method for producing a response upon receiving a particular INPUT. The response is obtained by utilizing the INPUT and a secret key. In the case of the present invention, the secret key is not stored within the memory of the smart card. Instead, the memory of the smart card is used to store a key-specific number (RND) and a coded or encoded key (A') where the coded key has been calculated using the secret key, the key-specific number and a second predetermined function. When the smart card receives an INPUT, the smart card reads the key-specific number and the coded key from its memory. The smart card, itself, then calculates the secret key using the retrieved key-specific number and the retrieved coded key by using the inverse function of the second predetermined function. Once the smart card has calculated the secret key, the smart card utilizes the calculated secret key, the received INPUT and a first predetermined function to produce a response for comparison with another response determined by a system with which the smart card is in communication and from which the smart card receives the INPUT. The applicant submits that by not storing the secret key within the memory of the smart card it is more difficult for the secret key to be obtained, thereby providing greater security for the smart card and a smart card user.

The Herve patent discloses a system including a portable object (1) such as a credit card which comprises at least one memory (3) associated with a processing means (4) which may be a microchip embedded in the credit card. The card is adapted to communicate with a facility (2) which includes a processing means (5), a memory (6), a comparator (8) and other components. In use, the credit card is inserted into a suitable card receiving adapter provided in the facility which causes the reading of an identification code from the memory of the credit card. If the identification code is plausible, a random number is generated within the facility and is transmitted to the card. The processor within the facility then calculates a number which is a function of a secret code stored within the facility. At the same time, the processor of the card calculates a number which is a function of the same secret code which is stored within the memory of the card. The facility then compares the two generated numbers and if they match, access to the facility is granted to the holder of the card. As correctly observed by the Examiner, the Herve patent fails to disclose, teach or suggest that the secret code be stored within the credit card in a coded or encoded manner. As also correctly observed by the Examiner, the Herve patent does not disclose, teach or suggest that a key-specific number could or should be stored within the memory of the smart card.

The Dolan *et al.* patent discloses a data communications system in which messages are processed using public key cryptography and a private key unique to one or more users under the control of a portable security device such as a smart card, held by each user. The system includes a server (130) for performing public key processing using the private key. The server stores or has access to the private key for each user in an encrypted form only. The private key is encrypted with a key encrypting key and each smart card comprises means for storing or generating the key encrypting key and providing the key encrypting key to the server. In use, in the Dolan *et al.* system, a person inserts a smart card into a reader associated with a work station (110) which is connected through a network to a powerful server (130) or a mainframe computer (140). Although it is not completely clear from the Dolan *et al.* patent, the smart card apparently does not have processing power or does not have sufficient processing power in order to perform the necessary functions for authenticating the smart card. Instead, Dolan *et al.* discloses that the powerful server computer (130) is used to assist the smart card in performing the necessary processing (see column 2, lines 12-16 and 54-64). Although the Dolan *et al.* patent suggests that a private key (coded key) be stored within the memory of the smart card, the Dolan *et al.* patent clearly does not teach or suggest that the smart card itself be employed for performing the necessary processing steps for authentication purposes.

It is respectfully submitted that the Examiner has failed to make a *prima facie* showing, which would support an obviousness rejection of claims 9-16. As noted above and as observed by the Examiner, the Herve patent fails to disclose, teach or suggest in any way that the memory of a smart card or credit card should contain either a coded key or a key-specific number. Instead, Herve teaches away from the present invention and specifically discloses that the actual secret key (S) be stored within the memory of the card and that the card perform the needed calculations. On the other hand, the Dolan *et al.* patent specifically teaches that it is advantageous to use a powerful server computer in order to assist a portable security device or card to perform the necessary processing for authentication. Accordingly, it is respectfully submitted that a person skilled in the art, who is trying to provide a more secure solution for handling a secret key in connection with a smart card would not consider the Dolan *et al.* patent because the Dolan *et al.* patent specifically teaches that a smart card should not have the necessary processing capability to produce, itself, a desired response. Instead, the Dolan *et al.* patent specifically teaches away from the concept of utilizing a smart card having sufficient processing power by its particular use of the external powerful server computer. Accordingly, it is respectfully submitted that a person skilled in the art would not be likely to combine the teachings of Herve and Dolan *et al.* to arrive at the claimed invention without utilizing hindsight. In particular, if one were to combine the teachings of Herve and Dolan *et al.* one would end up with a system in which the smart card would have insufficient processing power to, itself, generate the necessary authentication response.

In view of the foregoing, it is respectfully submitted that new claims 9-16 distinguish patentably over the combination of Herve and Dolan *et al.* and is respectfully submitted that claims 9-16 should be allowed.

Deleted claims 3 and 5 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Herve patent and Dolan *et al.* patent as applied to the other claims and further in view of International Publication No. W099-35782 (Kocher). The Examiner states that the Herve and Dolan *et al.* patent failed to teach a device which includes coding means for calculating a new coded key by means of the secret key, a new key-specific number to be fed to the coding means and the second predetermined function and a device which comprises means for replacing the coded key and the key-specific numbers stored in the memory with the new coded key calculated by the coding means and the new key-specific number. The Examiner takes the position that Kocher teaches these features and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate these features of Kocher into a system comprised of the Herve and Dolan *et al.* patents. For the reasons as set forth above, the applicant respectfully traverses this rejection as applied to any new claims 9-16.

As set forth in detail above, the Examiner has failed to make a *prima facie* case for combining the teachings of the Herve and Dolan *et al.* patents. It is respectfully submitted that the Kocher reference does not provide any teaching or suggestion to support either the combination of the Herve and Dolan *et al.* patents or the further combination of the Herve and Dolan *et al.* patents with the Kocher reference. It is therefore respectfully submitted that claims 9-16 distinguish patentably over the triple reference combination suggested by the Examiner.

In view of the foregoing amendment and discussion it is respectfully submitted that the present application, including claims 9-16, is in condition for allowance and such action is respectfully solicited.

Respectfully submitted,

LAURI PAATERO

June 7, 2005 By:
(Date)

LESLIE L. KASTEN, JR.
Registration No. 28,959
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1290
Facsimile: 215-965-1210
E-Mail: lkasten@akingump.com

LLK/nywp:lcd